UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Dropbox Account # 681053338,
That is stored at premises controlled by Dropbox, Inc.

Case No. 3:18SW8

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Eastern District of Virginia *(identify the person or describe property to be searched and give its location):* See "Attachment A"

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*: See "Attachment B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. § 2252A, and the application is based on these facts: See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Farris L. Moore, Special Agent, HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: January 16, 2018

/s/
David J. Novak
United States Magistrate Judge

City and state: Richmond, Virginia

Printed name and title

IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF VIRGINIA

Richmond Division

IN THE MATTER OF THE SEARCH OF: Dropbox, Inc. Account# 681053338	Case No. _____

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Farris Moore, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the account number 681053338 (hereafter "Target Account") that is stored at premises controlled by Dropbox, Inc. (hereafter Dropbox), an electronic service provider headquartered at 333 Brannan Street in San Francisco, CA 94107. The information to be searched is described in the following paragraphs and in Attachment A, incorporated herein by reference. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Dropbox to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent of the Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), currently assigned to the Office of the Assistant Special Agent in Charge Norfolk, in the Richmond, Virginia Office. I have been a Special Agent since 2001. As part of my daily duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defines in 18 U.S.C. § 2256(8)) in all forms of media including computer media. I have also spoken with other law enforcement agents concerning this matter. I make this application for a search warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure, and 18 U.S.C. § 2703(a) and (b), by which a court with jurisdiction over the offense may require the disclosure by a provider with electronic communication service of the contents of a wire or electronic communication.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2252A, specifically possession, receipt and distribution of child pornography have been committed by the Target Account. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband or fruits of these crimes further described in Attachment B, incorporated herein by reference.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." *See* 18 U.S.C. § 2711(3)(A)(i).

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

6. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Drobox to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

7. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

RELEVANT CRIMINAL STATUES

8. **Distribution or Receipt of Child Pornography**: 18 U.S.C. § 2252A(a)(2) provides that it is a crime to knowingly receive or distribute any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

9. **Child pornography** means any visual depiction, in any format, of sexually explicit conduct where: (A) the production involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital or computer-generated image that is substantially indistinguishable from that of a minor engaged in sexually explicit conduct; or (C) such visual

depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexual explicit conduct. *See* 18 U.S.C. § 2256(8).

10. **Visual depictions** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which are capable of conversion into a visual image, and data which are capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. *See* 18 U.S.C. § 2256(5).

11. **Sexually explicit conduct** means actual or simulated: (i) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

12. **Minor** means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

PROBABLE CAUSE

13. On August 15, 2017, law enforcement officials in Australia commenced an investigation of an Australia-based user of Kik Messenger ("Kik"), a freeware instant messaging mobile application, with the user name "ausdrover" for disseminating child exploitation material to other users. Notably, officers discovered chats between "ausdrover" and another Kik user named "lilglove1."

14. On August 18, 2017, "lilglove1" contacted "ausdrover" via Kik at 5:20:01 PM UTC and offered to trade "personal stuff."

15. On August 19, 2017, "ausdrover" sent one image labeled "fcdbd8fb-a137-4a52-acc1-526a94f55adb-preview" (Image#1) to "lilglove1." Image#1 depicts a white, female minor between the ages of 10 and16 years of age performing oral intercourse upon an unidentified adult, white male.

16. On August 19, 2017, "lilglove1" accordingly sent one image labeled "d08487fb-a188-4740-8020-a371a3249c9c-preview" (Image#2) to "ausdrover." Image#2 depicts an adult male hand exposing the vagina of a female minor between the ages of 2 and 10 years of age.

17. Subsequently, on August 23, 2017, law enforcement officials located and arrested the Australian Kik user "ausdrover" for distributing child pornography.

18. On August 24, 2017, Australian officials sent an emergency disclosure request to Kik Interactive Inc., the owner of Kik, for subscriber information associated with the "lilglove1" account. According to Kik Interactive, Inc., "lilglove1" had accessed the Kik application from IP address 73.31.192.7 from August 16, 2017 through August 21, 2017 on multiple occasions. In addition, Kik provided an associated email address for "lilglove1's" account, which was "lilglove@yandex.com." Using publicly available Internet tools, Australian officials discovered the suspect IP address originated from the Richmond, Virginia, area and subsequently referred it to HSI officials.

19. On November 7, 2017, your applicant sent a summons to Comcast requesting subscriber information for IP address 73.31.192.7 as part of its investigation into the receipt and distribution of child pornography. According to Comcast, the IP address 73.31.192.7 was assigned to James Burke during the August 16, 2017 to August 21, 2017, timeframe at 18408 Depot Road, McKenney, Virginia, which is located within the Eastern District of Virginia. Comcast also provided the email address "skooter77@comcast.net," which was associated with the account.

20. Further investigation revealed the presence of a secured Wi-Fi network in the area of 18408 Depot Road named "skooter."

21. Additionally, on or about November 13, 2017, the Internet storage service Dropbox reported to the National Center for Missing and Exploited Children (NCMEC) their discovery of

234 uploaded images and videos of suspected child pornography by Dropbox account user John Smith (681053338) with the email address "lilglove@yandex.com" from IP address 73.31.192.7.

22. On December 20, 2017, I reviewed one of the images provided to NCMEC by Dropbox. The image with file name "937542ce-42bb-41a9-8a5e-aea9562c1ca3.jpg" (Image# 3) depicts a male and a female, both between the ages of 10 to 18 years of age, naked and engaging in sexual intercourse.

23. On December 20, 2017, I reviewed one of the videos provided to NCMEC by Dropbox. The video with the file name "145999733548.mp4" (Video #1) depicts a shirtless minor male between the ages of 2 and10 years of age fondling the penis of an adult male, followed by the adult male ejaculating onto the chest of the minor.

BACKGROUND CONCERNING DROPBOX

24. In my training and experience, I have learned that Dropbox is a file syncing and collaboration service that allows users to access and share their files on computers, phones, tablets, and the Dropbox website. Subscribers obtain an account by registering with Dropbox. During the registration process, Dropbox asks subscribers to provide basic personal information. Therefore, the computers of Dropbox are likely to contain user content. In my training and experience, such content may constitute evidence of the crimes under investigation because the content can be used to identify the account's user or users.

25. Dropbox subscriber can also store with the provider files containing images, videos, contact or buddy lists, and other files, on servers maintained and/or owned by Dropbox.

26. In my training and experience, electronic service providers generally ask their subscribers to provide certain personal identifying information when registering for a Dropbox account. Such information can include the subscriber's full name, physical address, telephone numbers

and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

27. In my training and experience, electronic service providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.,* session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, electronic service providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the electronic service provider account.

CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

28. Through my discussions with law enforcement officers who specialize in the investigation of child pornography, and of subjects who use the Internet to gain access to child pornography, I have learned that individuals who use such technology are often child pornography collectors who download images and videos of child pornography.

29. Moreover, I have learned that many subjects have saved numerous images to their hard drive, thumb drive, disks or CDs, and have kept that material for long periods of time. Based upon my knowledge, experience, and training in child pornography

investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography.

30. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, in other visual media or from literature describing such activity.

31. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, drawings, or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

32. Collectors of child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, videotapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

33. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years

and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

34. Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

35. Collectors of child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

CONCLUSION

36. Based on the forgoing, I request that the Court issue the proposed search warrant and notice preclusion order. Because the warrant will be served on Dropbox who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Farris L. Moore, Special Agent
Department of Homeland Security
Homeland Security Investigations
Richmond, VA

SEEN AND APPROVED BY:

Samuel E. Fishel
Special Assistant United States Attorney

SUBSCRIBED and sworn before me on January 16, 2018.

/s/
David J. Novak
United States Magistrate Judge

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Account to be Searched

This warrant applies to all content within Dropbox account 681053338 (without limitation), to include all previously-preserved data under tracking number CR-6000-4510 that is or was stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., a company whose custodian of records is located at 333 Brannan Street, San Francisco, CA 94107

ATTACHMENT B

Particular Things To Be Seized

I. Items to be disclosed by Dropbox, Inc.:

To the extent that the information described in Attachment B is within the possession, custody, or control of Dropbox, Inc., Dropbox, Inc. is required to disclose the following information to disclose the following information (from inception to present) to the government for the account listed in Attachment A:

- All stored content stored or that was stored in the account, including copies of images, videos, spreadsheets, and any other files uploaded to Dropbox;
- All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of services utilized, the IP address used to register the account, log-in IP addresses associated with session times, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and sources of payment (including any credit or bank account number);
- All records or other information stored by an individual using the account, including address books, contacts, buddy lists, pictures and files;
- All records pertaining to communications between Dropbox Inc. and any persons regarding the account, including contacts with support services and records of actions taken;

- All records related to the users associated with Dropbox account number 681053338.

II. Information to be seized by the government:

All information described above in Section I and content that constitutes fruits, evidence and instrumentalities of violations of violation of 18 U.S.C. §§ 2251, 2252 and 2252A including, for user IDs identified on Attachment A, information pertaining to the following matters:

- Content in Dropbox account 681053338;
- The attempted or actual production, receipts, distribution and possession of child pornography; and
- Records relating to who created, used, or communicated with the user accounts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Dropbox and my official title is _____. I am a custodian of records for Dropbox. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Dropbox, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Dropbox; and

c. such records were made by Dropbox as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature